Gestion d'identités PSL – Exploitation IdP Authentic

Entr'ouvert SCOP – http ://www.entrouvert.com

Table des matières

1 Arrêt et démarrage

Authentic est démarré lors du boot de la machine et arrêté lors d'un shutdown. En dehors de ces moments, les commandes suivantes sont disponibles :

- `service authentic2 status` : état du service
- `service authentic2 stop` : arrêt du service
- `service authentic2 start` : démarrage du service
- `service authentic2 restart` : arrêt puis redémarrage du service

2 Configuration

2.1 Intégration à la fédération

Le choix de la fédération dans laquelle enregistrer l'IdP est fait dans le fichier `/etc/authentic2/supann.conf` (se référer au manuel d'installation pour plus d'information).

Une mise à jour des meta-données de la fédération est effectuée chaque heure, à XXh30, voir `/etc/cron.d/authentic2-supann`.

Cela signifie que l'ensemble de la configuration de tous les services (fournisseurs SAML) est faite dans les fichiers XML diffusés par la fédération (meta-données et filtre d'attributs). Si une modification locale de configuration est effectuée dans Authentic, elle sera écrasée par la mise à jour suivante.

2.2 Mise à jour forcée des données de la fédération

Lors de l'installation d'une nouvelle ressource dans la fédération, il peut être utile de mettre à jour aussitôt les méta-données au niveau de l'IdP sans attendre une heure. Pour cela, utiliser la commande suivante :

```
# su -s /bin/sh -c /usr/lib/authentic2-supann/update-renater-meta.sh authentic
```

Explication : cette commande lance le script `/usr/lib/authentic2-supann/update-renater-meta.sh` en tant qu'utilisateur `authentic`. Il s'agit de la commande qui est lancée chaque heure par cron, comme indiqué dans `/etc/cron.d/authentic2-supann`.

3 Charte graphique

3.1 Gabarits HTML, généralités

Pour définir la charte graphique du site, il faut créer des templates, c'est-à-dire des gabaris ou modèles de pages qui seront utilisés par Authentic pour construire les pages HTML.

Ces fichiers sont gérés par le moteur de rendu de Django. Pour savoir les utiliser, il faut connaitre leur langage de programmation, documenté ici : https://docs.djangoproject.com/fr/1.7/topics/templates/

Les gabarits par défaut sont installés dans le répertoire `/usr/share/pyshared/authentic2/templates/`. Ils ne doivent pas être modifiés, mais peuvent être replacés/surchargés.

Pour surcharger/remplacer un des gabarits par défaut, il faut créer un fichier avec le même nom, et dans le même sous-répertoire, à l'intérieur de `/var/lib/authentic2/templates/`.

Par exemple s'il faut surcharger `/usr/share/pyshared/authentic2/templates/authentic2/base.html` alors il faut créer un fichier `/var/lib/authentic2/templates/authentic2/base.html`.

3.2 Gabarit général : base.html

Un **gabarit de base** défini le style général du site, il est la base de toutes les autres pages. Il est écrit sur `/usr/share/pyshared/authentic2/templates/authentic2/base.html`.

Pour modifier le style général du site, il suffit de partir de ce fichier `base.html`, donc d'abord en faire une copie de travail :

```
# cp /usr/share/pyshared/authentic2/templates/authentic2/base.html \
                /var/lib/authentic2/templates/authentic2/base.html
# chmod 644 /var/lib/authentic2/templates/authentic2/base.html
```

Puis travailler sur le fichier obtenu `/var/lib/authentic2/templates/authentic2/base.html`

Les modifications opérées sur le gabarit sont immédiatement visibles sur le site. Cependant il se peut que différents systèmes de cache interviennent, auquel cas il peut être plus rapide de redémarrer Authentic (`service authentic2 restart`).

3.3 Fichiers statiques (images, css, js)

Les garabits HTML peuvent faire appel à des fichiers statiques, avec deux syntaxes possibles :

```
<link rel="stylesheet" href="{{STATIC_URL }}psl/css/style.css" />
```

ou la syntaxe plus actuelle :

```
{% load staticfiles %}  <!-- au tout début du fichier HTML -->
...
<img src="{% static "psl/img/logo.png" %}">
```

Le fichier correspondant doit être présent dans le répertoire `/var/lib/authentic2/static/`, c'est à dire avec les deux exemples ci-dessus :

- `/var/lib/authentic2/static/psl/css/style.css`
- `/var/lib/authentic2/static/psl/img/logo.png`

Une fois les fichiers copiés dans ces répertoires, il faut utiliser l'outil de déploiement des fichiers statiques de Django pour qu'il les place dans un répertoire géré par le serveur Web (Apache ici). Pour cela, il suffit de relancer l'IdP, son démarrage intègre le déploiement des statics :

```
# service authentic2 restart
```

Pour en savoir plus, lire la documentation de référence sur la gestion des fichiers statiques par un logiciel Django : https://docs.djangoproject.com/en/1.7/howto/static-files/

4 Interfaces de gestion

4.1 Interface d'administration

L'intégration à la fédération Renater « fixe » la configuration de l'IdP. Il peut cependant être parfois utile d'aller vérifier que la configuration est correcte. Pour cela, se rendre sur :

```
https ://idp.exemple.fr/admin/
```

et se connecter avec un compte administrateur, par exemple l'identifiant `admin` et le mot de passe choisi lors du `newdb` sur le serveur LDAP.

Attention : cette interface est une vue quasi directe de la configuration des services et utilisateurs. Il ne faut pas modifier ces configurations. L'interface d'administration est activée uniquement à des fins de vérification et/ou déboguage.

Attention : l'intégration à la fédération remets la configuration de chaque service à zéro, chaque heure — par exemple les réglements d'attributs.

4.2 Interface simplifiée

Une interface de gestion simplifiée est également disponible à l'adresse :

```
https ://idp.exemple.fr/manage/
```

Ici encore cette interface n'est présente qu'à des fins de vérification. Elle est prévue pour une instance d'Authentic qui gère elle-même ses utilisateurs et ses services, ce qui n'est pas le cas ici : les utilisateurs sont gérés dans l'annuaire LDAP, le services sont configurés via les données de la fédération.

5 Données à sauvegarder

Configuration :

- `/etc` complet
- sinon, au moins `/etc/authentic2/`
- sinon, au moins la bi-clé `/etc/authentic2/key.pem` et `/etc/authentic2/cert.pem`
- `/var/lib/authentic2` complet, surtout si les gabarits ont été adaptés (sous-répertoire `templates` et `static`)

Données (base PostgreSQL) :

Il est inutile de dupliquer la base de données, elle n'est utilisée par Authentic que pour enregistrer les configurations des services providers, celles-ci étant obtenues via la fédération.

6 Mise à jour du logiciel

La mise à jour du système doit être effectuée aussi fréquement que possible, typiquement une fois par jour (mises à jour de sécurité Debian). Entr'ouvert informera aussi le projet en cas de mise à jour urgente de sécurité à effectuer sur les composants mis en jeu par la solution.

La procédure de mise à jour est la suivante, en **deux étapes**.

Mise à jour de la liste des logiciels disponibles sur les dépôts de la solution (Debian et Entr'ouvert) :

```
# apt-get update
```

Mise à jour des paquets qui ont une version plus récente que celle installée :

```
# apt-get upgrade
```

Il est possible que des versions futures de la solution nécessitent l'installation de nouveaux paquets, dans ce cas Entr'ouvert mettra à jour les dépendances de ses paquets et il faudra utiliser la commande suivante :

```
# apt-get dist-upgrade.
```

7 Débogage

7.1 Journaux (logs)

Authentic est, techniquement, un processus géré par `gunicorn`, celui-ci enregistre ses logs dans :

- `/var/log/authentic2/gunicorn-access.log` : accès au service
- `/var/log/authentic2/gunicorn-error.log` : autres messages qui, malgré le nom du fichier, ne sont pas que les erreurs mais aussi des informations sur le démarrage et l'arrêt, par exemple.

Apache enregistre également les logs d'accès au service via HTTPS, dans deux fichiers :

- `/var/log/apache2/authentic2-supann_access.log` : logs d'accès
- `/var/log/apache2/authentic2-supann_error.log` : logs d'erreurs

7.2 Echanges SAML

Authentic est un IdP qui utilise le protocole SAML 2.0 pour ses échanges sur la fédération Renater. La majeure partie du débogage se passe en général via l'écoute des échanges SAML 2.0 dans un navigateur client. Nous conseillons l'utilisation du navigateur Firefox avec l'extension SAML tracer : https://addons.mozilla.org/fr/firefox/addon/saml-tracer/.

7.3 Mode DEBUG

Si le déboguage doit se faire dans le logiciel lui-même, il est possible d'activer le mode `DEBUG` dans `/etc/authentic2/supann.conf` :

```
# extrait de /etc/authentic2/supann.conf :
export DEBUG=1
```

puis relancer le service :

```
# service authentic2 restart
```

De nombreuses informations de débogage sont alors présentes dans `/var/log/syslog`, qui peuvent s'avérer importantes en cas de problème lourd. Elles peuvent être demandées en cas d'appel au support de la solution.

Par ailleurs, en cas d'erreur (HTTP 400 ou 500), des messages d'erreur système complets et détaillés (traceback) sont affichés sur le navigateur.

Attention : **ne jamais fonctionner en production avec le mode DEBUG**. En effet, dans ce mode, le service peut afficher des traces d'erreurs qui divulguent des informations sensibles sur le navigateur des utilisateurs.

---

8 Historique du document

20150611 tnoel – restructuration, adaptations à Authentic 2.1.20+

20150217 tnoel – première version